Compliance with Bias-Free Policing and Public Safety Analytics Policies

As new security technologies are implemented, maintaining compliance with the Bias-Free Policing and Public Safety Analytics Policies is crucial. In accordance with these two policies, Metro has adopted comprehensive strategies involving training, transparency, accountability, data management, and community engagement, which are relevant to the technologies discussed in this report. These two policies are also closely aligned with the White House Blueprint on AI Bill of Rights (Attachment D).

As stated in Section 3 of the Bias-Free Policing Policy, all contracted law enforcement entities are required to adhere to non-discriminatory practices. Vendors coming on board as part of new security efforts will also be required to develop and implement clear guidelines to explicitly mitigate biased policing, with mechanisms in place to identify, report, and address complaints.

As part of implementing weapons detection systems, Metro will work closely with vendors to determine the extent to which these technologies need to be tailored to meet the agency's expectation of transparency and accountability and ensure security practices are fair, equitable, and free from bias as required in Section 3 of the Public Safety Analytics Policy.

Similarly, when it comes to the collection, retention, and use of data in deploying resources, Metro will work to ensure internal procedures and those delegated to vendors, integrate diverse and representative validation and verification measures to avoid racial profiling and discrimination while holding personnel accountable for policy adherence as required in Section 3.7 of the Public Safety Analytics Policy and Section 3.2 of the Bias-Free Policing Policy.

As new security technologies are implemented, it is especially important to ensure personnel meet the training requirements in Section 3.3 of the Bias-Free Policing Policy. Equally important is the need for meaningful engagement and communication with stakeholders to build trust and foster strong relationships between Metro, law enforcement partners, and the public.

In terms of public safety analytics, ethical data usage has been paramount for Metro, following strong data governance policies and robust privacy protections. Analytics can assist in properly deploying emergency services, safety and security technology, and resources that improve the customer experience for all customers. Moving forward, and in compliance with Section 3.7 of Metro's Public Safety Analytics Policy, staff will work to offer transparency in the algorithms used by newly adopted technologies through education and regular impact assessments to continue to ensure fair outcomes.

In addition, conducting regular algorithmic audits, performing prompt software updates, and ensuring the use of diverse data sets will be critical to mitigating biases in analytics. These will be tracked through monitoring and Key Performance Indicators (KPIs) as outlined in Section 3.4 of Metro's Bias-Free Policing Policy. All future security technologies incorporated into the Metro ecosystem will adhere to these policies and practices.